Distributed Systems Security

Lab Assignments
Module 3: Fakebook part II (a)
IT Security Group

Guillermo Suárez de Tangil
(guillermo.suarez.tangil@uc3m.es)

Remembering module 1…

▶ **Firewall configuration**

  ▶ All users should have granted access to *Fakebook*

  ▶ The machine should have granted access to security updates

  ▶ Any other access should've not be granted

  ▶ Remote access and PING should be logged

  ▶ Remote connections only from a specific IP address

▶ **SSH**

  ▶ Remote administration (SSH)

▶ **File-system Permissions**

  ▶ New web administrator user

▶ **Denial of Service detection by means of Snort's IDS**

University Carlos III of Madrid
SeTI Group · Computer Sciencie Dept.

Distributed Systems Security – Lab Assignments

2

▸ **Web Server**

    ▸ Fakebook should be accessible for any user

    ▸ Tomcat's configuration should allow the correct operation of the web application

    ▸ Not reveal any critical information.

    ▸ SSL

▸ **Data Base**

    ▸ Accessible only from the local machine

    ▸ Web admin only tables related to the web.

Practical Assessment

- Deadline: December the 14th, 2011
- Deliveries:
  - Written report, scripts and configuration files
  - Outline
    - Security analysis
    - Security vulnerabilities
    - Vulnerability risk: **Information Assurance** vs. **Information Availability**
    - Vulnerability exploitation
    - Countermeasures and BCP (*justifying decisions taken*)
- Oral and Written Assessment (Operation)
  - Assessment process
    - White box testing: Manual evaluation of each VM
    - Black box testing: Automatic scripts
  - Pair Assessment
- Written Assessment (Knowledge)
  - Individual test

Tips and Useful Advises

▸ Analyze expected Server's workload

▸ Divide and conquer

    ▸ Break the module down (smallest work scopes)

▸ Before implementing, **abstraction**!

    ▸ Textual description of the changes to tackle

▸ Backup copies

▸ Criticize your own decisions

▸ Discuss in with other pairs

    ▸ **Do not plagiarize! (Knowledge assessment)**

References

- Assignment description
- Documentation Tomcat
  - Don't forget Google
- Documentation MyQSL
  - Also in Google